



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,238	04/01/2000	Srinivas Chaganty	M-8403 US	9955

7590

06/30/2005

David Volejnicek, Esq.
Avaya Inc.
307 Middletown-Lincroft Road
Room 1N-391
LINCROFT, NJ 07738

EXAMINER

HA, LEYNNA A

ART UNIT	PAPER NUMBER
----------	--------------

2135

DATE MAILED: 06/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

MAILED
JUN 3 0 2005
Technology Center 2100

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

**BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES**

Application Number: 09/540,238
Filing Date: April 01, 2000
Appellant(s): CHAGANTY ET AL.

Avaya Inc. – David Volejnicek, Esq.

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 24, 2005.

(1) Real Party in Interest

Avaya Technology Corp., the assignee is CyberIQ Systems and the inventors for this application are Bommareddy, et al.

(2) Related Appeals and Interferences

None

(3) Status of Claims

Claims 1-22 and 47-56 are allowed.

This appeal involves claim 23-46 and 57-63.

Claims 23-46 and 57-63 remains rejected.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is substantially correct. The changes are as follows:

After consulting and reviewing the issues brought up by Appellant in the Appeal, claims 1-22 and 47-56 are allowed. However, claims 23-46 and 57-63 remains rejected 35 U.S.C 102(e) over Coile, et al. (US 6,108,300), because independent claims 23, 40 and 57 fails to include the allowable features as claimed in the allowable claims 1, 16, and 47.

(7) Grouping of Claims

The rejection of claims 23-46 and 57-63 stand or fall together because appellant's brief does not include a statement that this grouping of claims does not stand or fall together and reasons in support thereof. See 37 CFR 1.192(c)(7).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct. There are typographic errors on "request" (claim 40, line 9) and "firewall" (claim 47, line 13).

(9) Prior Art of Record

6108300	Coile, et al.	8-2000
5828833	Belville, et al.	10-1998

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

A.) *Claims 23-30, 37-39, 40-46, and 57-63 are rejected under 35 U.S.C. 102(e) in view of Coile, et al. (US 6,108,300).*

As per claim 23:

Coile, et al. teaches a method and apparatus comprises a plurality of firewalls in the form of variety of network devices **300, 310** (FIG.2) or servers **210, 220** (FIG.1). The primary firewall is in the active state so it has the active MAC address and the backup (second) firewall is in standby status that has a different MAC address (col.10, lines 37-38). Coile's invention utilizes a switch circuit (or failover cable) plugged on each side of the firewalls (col.2, lines 50-58) to detect when a failure of a firewall occurs (col.5, lines 7-12). Once a failure is detected in the primary firewall, the MAC address of the primary firewall is changed to the MAC address of the backup (second) firewall in the packet header (col.2, line 64-col.3, line 2 and col.5, lines 55-61).

As per claim 24: See col.5, lines 26-31; discussing the plurality of servers.

Art Unit: 2135

As per claim 25: See col.2, line 64-col.3, line 2 and col.12, lines 10-23; discussing the switch circuit in the form of a failover cable is further configured to relay the packet to the second firewall after changing the a fixed MAC address of the first firewall to the fixed MAC address of the second firewall.

As per claim 26: See col.8, line 58-col.9, line 4; discussing the failover cable is configured to detect a failed firewall by transmitting a request to the first and second firewalls, wherein an absence of a reply from a particular firewall of the first and second firewalls is indicative of a failure of the particular firewall.

As per claim 27: See col.11, lines 2-8; discussing the failover cable is configured to detect a failed firewall by sending ARP requests to the first and second firewalls, wherein an absence of a reply to an ARP request from a particular firewall of the first and second firewalls is indicative of a failure of the particular firewall.

As per claim 28: See col.6, lines 16-20; discussing the failover cable is configured to detect a failed firewall by sending ICMP echo requests to the first and second firewalls, wherein an absence of a reply to an ICMP echo request from a particular firewall of the first and second firewalls is indicative of a failure of the particular firewall.

As per claim 29: See col.11, lines 3-; discussing the failover cable is configured to detect a failed firewall by monitoring responses from the firewalls to requests sent at predetermined intervals.

As per claim 30:

Coile discusses the switch circuit is configured to detect an address resolution protocol (ARP) request from the server to the first firewall (col.11, lines 2-8 and 55-65) and respond to the ARP request with the fixed MAC address of the second firewall, whereby the server sends the subsequent outbound packets with the fixed MAC address of the second firewall (col.12, lines 18-23).

As per claim 37: See col.6, lines 14-19 discussing transferring the packets between the server and a firewall.

As per claim 38: See col.7, lines 35-52 discussing full duplex between the firewall and the server.

As per claim 39: See col.13, line 8.

As per claim 40:

Coile, et al. teaches a method and apparatus comprises a plurality of firewalls in the form of variety of network devices or servers. Coile's invention detects when a failure of a firewall occurs (col.2, lines 50-58) by sending confirmation message across the network to indicate that the firewall has not failed or the firewall has failed (col.6, lines 38-67). In addition, Coile discloses processing an absence of a reply from the second side of the request message as a failure of the first firewall (col.8, line 58-col.9, line 4). Once a failure is detected in the primary firewall, the backup firewall becomes active (col.6, line 67 thru col.7, line 9), hence, replacing the fixed MAC address of the first

firewall with the fixed MAC address of the second firewall (col.5, lines 55-61 and col.12, lines 48-50) which it is necessary for the MAC address of the primary firewall is changed to the MAC address of the backup (second) firewall in the packet header (col.2, line 64-col.3, line 2).

As per claim 41: See col.13, lines 12-21 and FIG.9; discussing the first memory on said first side a first functional status for each firewall and the second memory on the second side a second functional status for each firewall wherein the first functional status is identical to second functional status.

As per claim 42: See col.13, lines 12-21; discussing maintaining each session information between computers separated by the firewall.

As per claim 43:

Coile teaches once a failure is detected, an active MAC address of a functional backup network device replaces the MAC address of the failed network device (col.6, line 67 thru col.7, line 9). Coile fails to suggest sending a request message to a second side of the firewall. It is inherent if Coile can send a request message through the firewall by having the MAC address, then it is possible to send a request message by using the MAC address to get to the location or to any side of the firewall. See Fig.1

As per claim 44: See col.6, lines 43-59; discussing the failover cable generates, sends, and processes.

As per claim 45: See col.5, lines 60-61 and col.6, lines 45-59; discussing performing the Network Address Translation (NAT) in the first firewall and

Art Unit: 2135

adding a rule in the first firewall to maintain unchanged an internet protocol (IP) address of a source of the request message.

As per claim 46: See col.10, lines 39-42; discussing receiving a request on a port and sending a replying said port.

As per claim 57:

Coile, et al. teaches a method and apparatus comprises a plurality of firewalls in the form of variety of network devices or servers. Coile's invention detects when a failure of a firewall occurs (col.2, lines 50-58) by sending confirmation message across the network to indicate that the firewall has not failed or the firewall has failed (col.6, lines 38-67). Once a failure is detected in the primary firewall, the backup firewall becomes active (col.6, line 67 thru col.7, line 9), hence, replacing the fixed MAC address of the first firewall with the fixed MAC address of the second firewall (col.5, lines 55-61 and col.12, lines 48-50) which it is necessary for the MAC address of the primary firewall is changed to the MAC address of the backup (second) firewall in the packet header (col.2, line 64-col.3, line 2).

As per claim 58: See col.7, lines 36-52; discussing the switch circuit performs detection.

As per claim 59: See FIGURES 7 and 8; discusses receiving the packet after detecting the failure and prior to the replacing.

As per claim 60: See FIGURE 4; transferring a plurality of packets other than the packet, between a host and a firewall in the plurality of firewalls through a switch circuit.

As per claim 61: See col.12, lines 29-31; discussing each of the packets contains a first IP address and the method does not change the first IP address during transferring of the packets to any of the firewalls.

As per claim 62: See col., lines 59-65; discussing each of the firewalls has a first side and a second side and each of the firewalls has the first IP address on the first side and a second IP address on the second side.

As per claim 63: See col.5, lines 55-65; discussing the method does not change the MAC address of any of the packets during the transferring, until the detecting of failure.

B.) Claims 31-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coile, et al. and further in view of Belville, et al. (US 5,828,833).

As per claim 31:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no

response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

As per claim 32:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable waiting for a time out period to pass (col.6, lines 36-63) (col.6, lines 56—63).

Art Unit: 2135

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of, Bellville, within the system of Coile, because when the time out passes the privileges are allocated so the packet is not transferred to the non-operational firewall.

As per claim 33:

The same rationale applies to claim 32, and further includes the time out period is greater than or equal to a time period needed for the recovered firewall to learn routes to all the known clients. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of, Bellville, within the system of Coile, because it is more secure by having the advantage to have enough time and not less than the time period to learn the routes to all known clients. Else, there is no point for the recovered firewall to operate as securely as before. See col.5, lines 3-9 and col.12, lines 47-53.as rejected on the same basis as claim 10.

As per claim 34:

The same rationale applies of claim 31, and further includes where Belville discusses periodically pinging the firewall application to see if it is still operational. The Examiner asserts if the failed firewall receives a ping and responds, then that is an indication the firewall has recovered and is functional once again. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of, Bellville,

within the system of Coile, because it is an indication that the firewall has regained its operational state. See col.6, lines 36-55.

As per claim 35:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17). See col.6, lines 36-55.

As per claim 36:

Coile teaches a method and apparatus for providing a failover for network devices such as firewalls by sending confirmation messages, ARP

request, and ping (ICMP) tests to each of the network devices and if there is no response, then that network device has failed. However, Coile fails to provide a recovery method for the failed firewall.

Belville, et al. teaches the method for proper recovery if there is a failure of the firewall (col.6, lines 54-55). In addition, Belville teaches the DCE firewall application includes a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of, Bellville, within the system of Coile, because the recovery method for the failed firewall would regain the operations of a functional firewall to continue to provide secure services of a network (col.4, lines 50-58 and col.5, lines 15-17).

(11) Response to Argument

As discussed in the section of Grouping of Claims, there is only one group of Claims 23-46, 57-63 and they are stand or fall together. Thus, Claim 57 is represent for this group.

Response to the section 102(e) rejection over Coile et al.:

Coile teaches in Claim 57, a network system having a switch from a network device 110 for sensing a failure has occurred (fault-tolerance), col. 2, lines 50-53. A primary MAC address coupled to the network device 110 and a back-up network device 120, which is connected to a backup MAC address. Coile discloses that a MAC address is an address of a device at the sublayer of the data link layer that deals with issues specific to a particular type of LAN. The MAC address is generally hardcoded into the device, which changes depending upon where it is plugged into the network, col. 5, line 66 - col. 6, line 13. Thus, Coile teaches that the primary MAC and backup MAC each has its own hardcoded (fixed) and different from each other because they are plugged into different locations of networks. Coile teaches when a failure is detected from the primary network device, it necessary to change, i.e., replace, the relevant packet header so that the packets are sent to the backup network device, col. 2, line 64 – col. 3, line 2. The primary network device enters a state of receiving configuration commands along the failover cable, and handling the packets in accordance with its configuration, col. 11, lines 60-65. The backup network device assumes the active MAC address. The failover cable is configured to monitor and to learn the new location of the active MAC address, col. 12, lines 48-50. Thus, Coile anticipates the claimed replacing, in a packet,

the fixed MAC address of the primary network device (first firewall) with the fixed MAX address of the backup network device (second firewall).

Appellant stated that the appealed claims require that individual firewalls have different and fixed MAC addresses, and MAC address of firewalls are swapped in packets and not between firewalls.

As discussed above, Coile teaches the MAC address is generally hardcoded into the device, which changes depending upon where it is plugged into the network, col. 6, lines 3-14. Thus, the primary MAC from the network device 110 and backup MAC from backup network device, each has its own hardcoded (fixed) and different address from each other because they are plugged into different locations of networks. Claim 57 recites replacing, in a packet, the fixed MAC address of the first firewall with the fixed MAC address of a second firewall in the plurality of firewalls. Evidently that Claim 57 does not recite "MAC address of firewalls are swapped in packets and not between firewalls", as appellant contended. Coile clearly anticipates this limitation by teaching that when the network device 110 fails (first firewall), the relevant packet headers are changed accordingly so that they are sent to the backup network device (second firewall), col. 2, line 65 – col. 3, line 2.

Appellant addressed that Coile et al explicitly state the two devices do swap their MAC addresses with each other. Appellants cited col. 1, lines 38-40, col. 6, lines 11-13, col. 7, lines 17-23, col. 10, lines 34-39, col. 12, lines 15-20, lines 41-44 for supporting this allegation.

Col. 1, lines 38-40 is in the Background of the invention in Coile, which provides general methods and apparatuses in a failover network before Coile's invention. Facts in the Background, i.e., prior art, are normally causes for being improved or modified by the present invention.

Appellant pointed in col. 6, lines 11-13, but appellant dropped the beginning of the sentence. The whole sentence is reproduced. In one embodiment of the present invention, the active MAC address is adopted by the active network device and is therefore not assigned to only one device. First, Coile teaches different embodiments not only one embodiment. Second, Coile teaches the active MAC address is adopted by the active network device. That means a MAC address is generally hardcoded into the device, which changes depending upon where it is plugged into the network, col. 6, lines 3-14. Thus, appellant's allegation of MAC address swaps between each other, namely, between the active network device and the backup network device, is irrelevant to the active MAC address is adopted by the active network device in Coile.

Col. 7, lines 17-23 disclose: "However, a problem could result if the former active device still responded to that MAC address. One problem would be that the switch might not be able to properly learn that the MAC address moved. Other ambiguities would likely occur. Since the former active device learns from the new active device that it failed, this is avoided and the former active device moves to the standby IP and MAC address". Again, appellant fails to point to the whole paragraph of this problem prediction in Coile. In

lines 14-17 of col. 7, Coile discloses that “assuming the MAC address is advantageous since clients do not have to ARP and find out the MAC address of the new active server before they can connect. However, a problem could result if”. Thus, Coile clearly teaches that assuming, i.e., replacing the MAC address is advantageous but raising a problem. In Coile, when the network device 110 fails (first firewall), the relevant packet headers (in MAC addresses) are changed accordingly so that they are sent to the backup network device (second firewall), col. 2, line 65 – col. 3, line 2.

Col. 10, lines 34-49, appellant cited different incomplete sentences in this citation on page 8 of the Appeal brief. In the same col. 10, Coile discloses on lines 32-38, that “each switch has associated with each physical connection the MAC address that it is on that connection. As noted above, when the active and standby network devices change state, they also change MAC address and IP addresses” (IP address is used for directing packets) and “Thus, the switch will momentarily detects that a network device with a different MAC address then it expects has been physically connected to it.” Thus, it is clear that packets are changed in the MAC address of the active network device with a different MAC address of the standby network device.

Col. 12, lines 15-20 state that “the backup device assumes the MAC address and the IP address of the active device.” As discussed above, each switch has associated with each physical connection the MAC address. This provides that each network device has its own MAC address. When the active

and standby network devices change state, they also change MAC address and IP addresses. By stating that the backup device assumes the MAC address and the IP address of the active device in the event of a failover cable, Coile anticipates the claimed replacing (is assuming, The Random House College, Dictionary, p. 1119) in a packet, the fixed MAC address of the first firewall with the fixed MAC address of a second firewall in the plurality of firewalls.

Appellant quotes the examiner from the Final rejection (pg.24), to have said “do not swap their MAC addresses” because “it would not be logical”. By looking on pg.24, the examiner in fact did not state any swapping of the MAC addresses but as quoting (a term from Coile) to “adopt” the MAC address of the active firewall. Further, the examiner stated in a continuous sentence that “it would not be logical if the failed firewall takes on an address of an active firewall leaving that firewall that is really active with no responsibilities.” The appellant have misconstrued “it would not be logical” by taking part of a sentence along with Appellant’s misinterpretation of “adopt” to become it would not be logical to swap the MAC addresses as what was said by the examiner.

Response to the section 103(a) rejection over Coile et al. in view of

Belville:

Belville, et al. teaches a similar invention as Coile that includes the method controlling traffic through the firewall but goes a further step by including proper recovery if there is a failure of the firewall (col.6, lines 54-55).

and a DCE firewall application which is a clean-up thread that periodically pings the servers to determine if the servers and firewalls are still present and operable (col.6, lines 36-49).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the teachings of the combined Coile and Belville does render the claimed invention unpatentable.

Claims 1-22, 47-56 are allowed. Coile or in combination of Belville fails to teach the claimed changing a MAC address of the packet to the fixed MAC address of a functional firewall of the plurality of firewalls when the packet is detected and relaying the packet to the functional firewall after the MAC address of the packet is changed.

Art Unit: 2135

Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

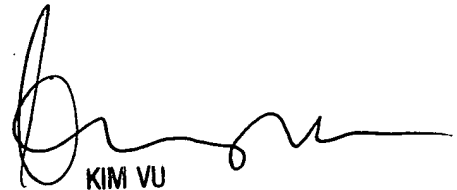


Leynna Ha
June 27, 2005

Conferees

Kim Vu - SPE *KV*

Hosuk Song - PE *HS*



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135

David Volejnicek, Esq.
Avaya Inc.
307 Middletown-Lincroft Road
Room 1N-391
LINCROFT, NJ 07738